Bipartite entangled stabilizer mutually unbiased bases as maximum cliques of Cayley graphs

Wim van Dam*
Department of Computer Science, University of California, Santa Barbara, CA 93106, USA
Department of Physics, University of California, Santa Barbara, CA 93106, USA

Mark Howard†
Department of Physics, University of California, Santa Barbara, CA 93106, USA
(Dated: January 19, 2013)

We examine the existence and structure of particular sets of mutually unbiased bases (MUBs) in bipartite qudit systems. In contrast to well-known power-of-prime MUB constructions, we restrict ourselves to using maximally entangled stabilizer states as MUB vectors. Consequently, these bipartite entangled stabilizer MUBs (BES MUBs) provide no local information, but are sufficient and minimal for decomposing a wide variety of interesting operators including (mixtures of) Jamiołkowski states, entanglement witnesses and more. The problem of finding such BES MUBs can be mapped, in a natural way, to that of finding maximum cliques in a family of Cayley graphs. Some relationships with known power-of-prime MUB constructions are discussed, and observables for BES MUBs are given explicitly in terms of Pauli operators.

PACS numbers: 03.65.Aa, 03.67.-a

I. INTRODUCTION.

One of the most important and long-studied tools in quantum information theory is that of mutually unbiased bases (MUBs). Two orthonormal bases $\mathcal{A} = \{|a\rangle\}$ and $\mathcal{B} = \{|b\rangle\}$ in a Hilbert space of dimension d are said to be mutually unbiased when $|\langle a|b\rangle| = 1/\sqrt{d}$ i.e. certainty of a measurement outcome in one basis implies complete uncertainty of a measurement outcome in another. This is the finite-dimensional analogue to the complementarity of position and momentum in continuous variable quantum mechanics. Typically, MUBs are most useful in Hilbert spaces, $\mathcal{H}_d$, of prime power dimension ($d = p^k$), for which *complete* sets of MUBs are known to exist and a number of construction methods are available. Ignoring the trace component (which is often known or unimportant), decomposing a $d \times d$ Hermitean operator (e.g. a density matrix) requires $d^2 - 1$ parameters, which necessitates measuring $d + 1$ different observables (since each observable yields $d - 1$ independent probabilities). Complete sets of MUBs are sets with $d + 1$ orthonormal bases, possessing the desirable properties of being both mutually unbiased with respect to one another and also being minimal in terms of the number of observables required (hence this is considered the optimal tomography set-up [1, 2]).

Our work here concerns the construction of MUBs in Hilbert space of dimension $d = p^2$ that are deliberately incomplete in that they contain only $p^2 - 1$ observables – insufficient for parameterizing all operators in $\mathcal{H}_{p^2}$, but sufficient and *minimal* for the description of Hermitean operators that are local maximally mixed (LMM) [3]. LMM operators, W, defined on a bipartite system $\mathcal{H}_{p^2} = \mathbb{C}^p \otimes \mathbb{C}^p$ are those for which $\mathrm{Tr}_1(W) = \mathrm{Tr}_2(W) \propto \mathbb{I}$. This class of operators is surprisingly broad. The Jamiołkowski isomorphism, for example, tells us that any unital map $\mathcal{E}$ acting on $\mathcal{H}_p$ can be represented by an LMM operator, indicating that this result could potentially be useful for the characterization of noise processes, whilst reducing the number of measurements required (process tomography using a similar construction is discussed in detail in [4]). Other scenarios in which the non-local information is of paramount importance include investigation of bipartite entangled and non-local states, and the witnesses [5] and Bell inequalities [6] that identify them. As a final example, the motivation for this work came in considering a convenient, minimal basis with which to decompose so-called Clifford witnesses for detecting stabilizer vs. nonstabilizer operations [7].

The literature concerning MUBs, constructions and related structures is vast. This field of study seems to originate with Schwinger's construction for unitary operator bases [9] in 1960, and subsequently Ivonovic's 1981 construction [10] for complete MUBs in prime dimensions. Wootters and Fields [2] provided a MUB construction for power-of-prime dimensions $d = p^k$ and showed its optimality for state reconstruction (tomography). A more recent (2002) construction that also works for power-of-prime dimensions is given by Bandyopadhyay *et al.* [11] and this is framed explicitly in terms of Pauli operators and stabilizer states. Lawrence *et al.* [12] found a similar construction for multi-qubit systems in the same year. Since then a large number of related results have been published e.g. [13–16] (also see a recent review article [17] and references therein) and a number of interesting connections with combinatorics (e.g. mutually orthogonal Latin squares [18]) and finite geometry [19–21]. A prominent example of the usefulness of MUBs is their optimality for state or process reconstruction (a recent experimental result [1] shows an improvement over standard techniques by using MUB state tomography). Quantum key distribution schemes [27, 28] typically rely on MUBs for their security. Another important application of MUBs is their interpretation in terms of finite phase space, leading to a discrete Wigner function; for a particular choice of MUB using stabilizer states, the resulting Wigner function can shed light on the computational power

* vandam@cs.ucsb.edu;
† mhoward@physics.ucsb.edu

of circuits in the so-called "Clifford computer" model [7, 22–24].

Inadvertently, we have rediscovered some results that were previously known in the context of quantum key distribution [28], and in the context of unitary designs [4, 29] (i.e., the Cliffords that we use to create some of our BES-MUBs are known to create a minimal unitary design). Recent work by Planat [30] is somewhat related to our current investigation, insofar as it utilizes graph theoretical concepts and stabilizer (Pauli operator) observables to examine the construction of MUBs. Kalev *et al.* [16] investigated MUBs in bipartite systems using sets of commuting Pauli operators, but their work is more focused on complete sets of MUBs for density operators in $\mathcal{H}_{p^2}$.

This work provides an alternative graph-theoretic method (as opposed to unitary designs or finite field constructions) of analyzing MUBs and similar structures in quantum information theory. It is hoped that a combination of the alternative methods outlined here, in addition to those of [4, 28–30] and others, will prove fruitful for further analyses. We show how to create an orthonormal basis of p^2 stabilizer states in $\mathcal{H}_{p^2}$, given a matrix $F \in SL(2,\mathbb{Z}_p)$. Furthermore, we show that the quantity $\mathrm{Tr}(F_i^{-1}F_j)$ indicates whether the bases corresponding to F_i and F_j are mutually unbiased. This leads naturally to a Cayley graph structure wherein graph vertices are given by the elements of $SL(2,\mathbb{Z}_p)$, and edges between vertices correspond to mutual unbiasedness of the corresponding bases. The BES MUBs that we seek are easily shown to be maximum cliques of the Cayley graphs, and for primes up to 11 we can partition $SL(2,\mathbb{Z}_p)$ into p distinct (non-overlapping) BES-MUBs. For primes 13 and higher, it is an interesting open question whether such BES-MUBs exist, as a deterministic search for the maximum clique is infeasible. For the related question of minimal unitary designs it has been noted by Chau that subgroups of $SL(2,\mathbb{Z}_p)$ of a particular size only exist for primes up to 11, but it is not clear that complete BES-MUBs depend in any way on the existence of such subgroups. The family of Cayley graphs under consideration (defined for all primes p) is actually the graph complement of a family of Ramanujan graphs, and we are able to list some general graph-theoretic properties that hold for all values of p. In section II we review the necessary background concerning the Clifford group and introduce some graph-theoretical concepts that will be useful in later sections. In section III we explicitly give the recipe for constructing BES-MUBs and relate our work to a well-known MUB construction that uses finite field methods. Section IV further explores the quantities and concepts from graph theory that can be applied to our family of Cayley graphs, and finally, Appendix A provides a description of the MUB observables in terms of stabilizer measurements as well commuting sets of Pauli operators.

II. DEFINITIONS AND USEFUL RESULTS

A. Relevant finite groups and their properties

The finite-dimensional analogues of position and momentum operators are denoted by X and Z, arbitrary products of which are called displacement operators D, indexed by a vector $u = (u_1, u_2) \in \mathbb{Z}_p^2$:

$$X|j\rangle = |j+1\rangle \quad Z|j\rangle = \omega^j|j\rangle \quad \left(\omega = e^{2\pi\imath/p}\right) \tag{1}$$

$$D_u = \tau^{u_1u_2} X^{u_1} Z^{u_2} \quad \tau = e^{(p+1)\pi\imath/p}. \tag{2}$$

The Weyl-Heisenberg group (or generalized Pauli group) for a single qupit is given by

$$\mathcal{G}_p = \left\{\tau^c D_u | u \in \mathbb{Z}_p^2, c \in \mathbb{Z}_p\right\}. \tag{3}$$

The set of unitary operators that map the Pauli group onto itself under conjugation is called the Clifford group (sometimes called the Jacobi group):

$$\mathcal{C}_p = \{C \in U(p) | U\mathcal{G}_p U^\dagger = \mathcal{G}_p\}.$$

The fact that every Clifford operation in dimension p can be associated with a matrix $F \in SL(2,\mathbb{Z}_p)$ in addition to a vector $u \in \mathbb{Z}_p^2$ results from the isomorphism

$$\mathcal{C}_p \cong SL(2,\mathbb{Z}_p) \ltimes \mathbb{Z}_p^2, \tag{4}$$

established by Appleby [32], where $\mathcal{C}$ is the Clifford group. If we specify the elements of F and u as

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2,\mathbb{Z}_p) \qquad u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \in \mathbb{Z}_p^2 \tag{5}$$

then Appleby provides an explicit description of the unitary matrix $C_{(F|u)} \in \mathcal{C}_p$ in terms of these elements i.e.,

$$C_{(F|u)} = D_u U_F \tag{6}$$

$$U_F = \begin{cases} \frac{1}{\sqrt{p}} \sum_{j,k=0}^{p-1} \tau^{\beta^{-1}\left(\alpha k^2 - 2jk + \delta j^2\right)} |j\rangle\langle k| & \beta \neq 0 \\ \sum_{k=0}^{p-1} \tau^{\alpha\gamma k^2} |\alpha k\rangle\langle k| & \beta = 0. \end{cases} \tag{7}$$

Note how composition and inverses can be represented in this notation [31]

$$C_{(F|u)} C_{(K|v)} = C_{(FK|u+Fv)} \tag{8}$$

$$C_{(F|u)}^{-1} = C_{(F|u)}^\dagger = C_{(F^{-1}|-F^{-1}u)} \tag{9}$$

We will have need to relate the matrix trace $\mathrm{Tr}\left(C_{(F|u)}\right)$ to the matrix trace $\mathrm{Tr}\,(F)$ modulo p:

$$|\mathrm{Tr}\left(C_{(F|u)}\right)| = \begin{cases} \in \{0, \sqrt{p}, p\} & \text{if } \mathrm{Tr}(F) = 2 \\ 1 & \text{if } \mathrm{Tr}(F) \neq 2 \end{cases} \tag{10}$$

To see why this is so we must define the Legendre Symbol

$$\ell_p(x) = \begin{cases} 1 & \text{if} \quad x \text{ is a quadratic residue} \pmod p \\ -1 & \text{if} \quad x \text{ is a quadratic non-residue} \pmod p \\ 0 & \text{if} \quad x \equiv 0 \pmod p. \end{cases}$$

and quote a result from Appleby [32]

$$(\text{ Case 1: } \quad \beta = 0 \Rightarrow \alpha \neq 0 \,)$$

$$|\mathrm{Tr}\left(C_{(F|u)}\right)| = \begin{cases} |\ell_p(\alpha)| = 1 & (\mathrm{Tr}(F) \neq 2) \\ |\ell_p(\gamma)|\sqrt{p}\delta_{u_1,0} & (\mathrm{Tr}(F) = 2, \gamma \neq 0) \\ p\delta_{u_1,0}\delta_{u_2,0} & (\mathrm{Tr}(F) = 2, \gamma = 0) \end{cases} \tag{11}$$

$$(\text{ Case 2: } \quad \beta \neq 0 \,)$$

$$|\mathrm{Tr}\left(C_{(F|u)}\right)| = \begin{cases} |\ell_p(\mathrm{Tr}(F) - 2)| = 1 & (\mathrm{Tr}(F) \neq 2) \\ |\ell_p(-\beta)|\sqrt{p}\delta_{u_2,\beta^{-1}(1-\alpha)u_1} & (\mathrm{Tr}(F) = 2) \end{cases} \tag{12}$$

Finally, we note some important facts regarding the structure of the group $SL(2,\mathbb{Z}_p)$. A minimal set of generators is e.g.

$$SL(2,\mathbb{Z}_p) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle \tag{13}$$

It has order $|SL(2,\mathbb{Z}_p)| = p(p^2-1)$ and can be partitioned into $p+4$ conjugacy classes [33], each of which has constant trace. If we partition $SL(2,\mathbb{Z}_p)$ by the matrix trace of its elements, $\mathrm{Tr}(F)$, we see the following

$$\left|\left\{F|\ell_p\left((\mathrm{Tr}(F))^2 - 4\right) = 1\right\}\right| = \quad p(p+1) \tag{14}$$

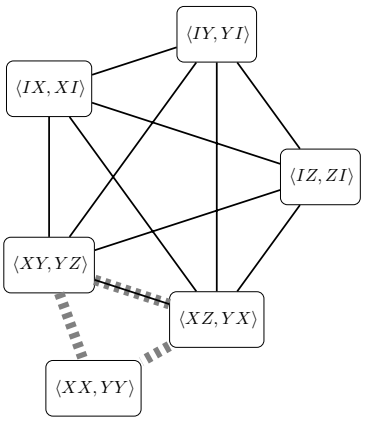
$$\left|\left\{F|\ell_p\left((\mathrm{Tr}(F))^2 - 4\right) = -1\right\}\right| = \quad p(p-1) \tag{15}$$

$$\left|\left\{F|\ell_p\left((\mathrm{Tr}(F))^2 - 4\right) = 0\right\}\right| = \quad p^2 \tag{16}$$

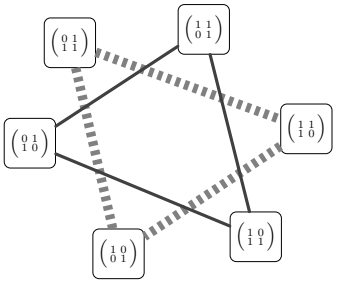
The final sets $\{F|\mathrm{Tr}(F) = 2\}$ and $\{F|\mathrm{Tr}(F) = -2\}$ are each comprised of three conjugacy classes. Many of these facts will be used in subsequent sections, particulary section IV concerning graph-theoretical properties of Cayley graphs that are relevant to the construction of BES MUBs.

B. Graphs: Cayley Graphs and Maximum Cliques

We review some relevant notation and properties of graphs that can be found in any standard reference (e.g, [34]). An undirected Cayley graph $\Gamma(G,T)$ with an associated finite group G and set $T \subset G$, is the graph whose vertices are the elements of G and whose set of edges is $\{g_1 \sim g_2 | g_1^{-1} g_2 \in T\}$. We must have $I \notin T$ and $T^{-1} = T$. The resulting graph $\Gamma(G,T)$ is regular i.e. each vertex has degree $|T|$, and the number of (undirected) edges is given by $\frac{1}{2}|G||T|$. A complete graph of order n, denoted K_n, is a graph with n vertices, each of which is adjacent to every other vertex (see Fig 1 (a) for an example K_5). A subgraph, Γ', of Γ, is a graph whose vertices form a subset of the vertices of Γ and the adjacency relation is inherited from Γ. A clique of Γ is a complete subgraph of Γ, where the size of the clique is given by the number of vertices in this subgraph. The largest possible clique (not necessarily unique) contained in Γ is a maximum clique, the size of which is usually denoted $\omega(\Gamma)$. We discuss graph-theoretic properties, and what they say about the problem at hand, in more detail in Section. IV.



(a)



(b)

FIG. 1. MUB structure: (a) MUBs in dimension 2^2. Each box represents a two-qubit stabilizer state $\rho = \frac{1}{4}\sum_{s\in\mathcal{S}} s$ where $\mathcal{S}$ is the abelian subgroup generated by the Pauli operators contained in $\langle\cdot\rangle$. Varying the signs of the generators creates a complete orthonormal basis from each representative pair. Lines between boxes indicate that the overlap between two states is $\mathrm{Tr}(\rho_a\rho_b) = \frac{1}{4}$. The solid lines depict the complete graph on 5 vertices, K_5, and this corresponds to a complete MUB on this Hilbert space. The dashed lines depict a triangle, K_3, which forms a BES MUB. (b) Two different BES MUBs (solid and dashed complete graphs K_3) that partition $SL(2,\mathbb{Z}_2)$, where each 2×2 matrix F corresponds to the Jamiołkowski state $(I\otimes C_{(F|0)})\sum_{j=0}^{j=1}|jj\rangle/\sqrt{2}$. Adjacent vertices $F_1, F_2 \in SL(2,\mathbb{Z}_p)$ satisfy $\mathrm{Tr}(F^{-1}F_2) \neq 2$, which in terms of the corresponding density matrices implies $\mathrm{Tr}(\rho_{(F_1)}\rho_{(F_2)}) = \frac{1}{4}$.

III. CONSTRUCTION OF THE RESTRICTED MUB

The goal is to create a set of states, $\mathcal{S}$, of size $|\mathcal{S}| = p^2(p^2-1)$ that is partitioned into p^2-1 subsets, where each subset, containing p^2 states, forms an orthonormal basis. Labeling the basis with a supercript and the individual states within a basis using a subscript we have

$$\mathcal{S} = \{|\psi_1^1\rangle \ldots |\psi_j^k\rangle \ldots |\psi_{p^2}^{p^2-1}\rangle\}.$$

This is a mutually unbiased basis if

$$|\langle\psi_j^k|\psi_m^n\rangle| = \frac{1}{p}(1-\delta_{k,n}) + \delta_{k,n}\delta_{j,m}.$$

The $|\psi_j^k\rangle$ of the set $\mathcal{S}$, that comprises our bipartite entangled stabilizer MUB (BES MUB), will be maximally entangled stabilizer states – formed by applying a Clifford operation, C, to one half of a maximally entangled state

$$|J_C\rangle = (I\otimes C)\sum_{j=0}^{p-1}\frac{|jj\rangle}{\sqrt{p}}.$$

The overlap $|\langle J_{C_m}|J_{C_n}\rangle|$ between any two such states is given by

$$|\langle J_{C_m}|J_{C_n}\rangle| = \frac{1}{p}|\mathrm{Tr}(C_m^\dagger C_n)|.$$

Using the notation we have previously described, it is easy to show using Eq.s $8-10$ that

$$\begin{aligned} &\text{if} \quad \mathrm{Tr}(F^{-1}K)\neq 2 \\ &\text{then} \quad \left|\mathrm{Tr}\left[\left(C_{(F|u)}\right)^\dagger\left(C_{(K|v)}\right)\right]\right| = 1 \quad \forall u,v\in\mathbb{Z}_p^2 \end{aligned} \tag{17}$$

i.e., a pair of matrices $F,K\in SL(2,\mathbb{Z}_p)$ satisfying $\mathrm{Tr}(F^{-1}K)\neq 2$ defines a pair of mutually unbiased basis. Since the subspace under consideration has dimension $(p^2-1)^2$, and since each basis contains p^2-1 independent states, we require a total of p^2-1 matrices $F_i\in SL(2,\mathbb{Z}_p)$, satisfying, pairwise, $\mathrm{Tr}(F_i^{-1}F_j)\neq 2$, in order to create the BES MUB.

Define

$$\begin{aligned} G &= SL(2,\mathbb{Z}_p) & |G| &= p(p^2-1) \\ T &= \{F\in SL(2,\mathbb{Z}_p)|\mathrm{Tr}(F)\neq 2\} & |T| &= |G|-p^2 \end{aligned} \tag{18}$$

then the Cayley graph $\Gamma(G,T)$ has the property that two vertices F_i and F_j are adjacent if and only if $\mathrm{Tr}(F_i^{-1}F_j)\neq 2$. A clique of size p^2-1, if it exists, immediately gives the desired complete BES MUB by the preceding discussion. Furthermore, a clique of size p^2-1 must be a maximum clique since the dimension of the Hilbert space for local maximally mixed operators is $(p^2-1)^2$.

Theorem 1 *A pair of matrices $F_1,F_2\in SL(2,\mathbb{Z}_p)$ satisfying $Tr(F_1^{-1}F_2)\neq 2$ defines a pair of mutually unbiased bases in $\mathcal{H}_{p^2}=\mathbb{C}^p\otimes\mathbb{C}^p$ (via the relationship between $SL(2,\mathbb{Z}_p)$ and the Clifford group). A set of matrices $\mathcal{F}=\{F_i\}$, of order $|\mathcal{F}|=p^2-1$, such that pairwise $Tr(F_i^{-1}F_j)\neq 2 \pmod p$, defines (i) a complete bipartite entangled stabilizer MUB (ii) a maximum clique of the Cayley graph defined in Eq. (18).*

One can check using a computer algebra system [37, 38] that the following subgroups $H_p\leq SL(2,\mathbb{Z}_p)$ have order $|H_p|=p^2-1$, and every pair of elements $F_i,F_j\in H_p$ satisfies $\mathrm{Tr}(F_i^{-1}F_j)\neq 2$ (i.e. these subgroups provide complete BES MUBs).

$$p=3: \quad H_3 = \left\langle \begin{pmatrix} 0 & 1\\ 2 & 0\end{pmatrix}, \begin{pmatrix} 1 & 1\\ 1 & 2\end{pmatrix}\right\rangle \tag{19}$$

$$p=5: \quad H_5 = \left\langle \begin{pmatrix} 0 & 2\\ 2 & 0\end{pmatrix}, \begin{pmatrix} 1 & 1\\ 2 & 3\end{pmatrix}\right\rangle \tag{20}$$

$$p=7: \quad H_7 = \left\langle \begin{pmatrix} 0 & 2\\ 3 & 0\end{pmatrix}, \begin{pmatrix} 1 & 1\\ 4 & 5\end{pmatrix}\right\rangle \tag{21}$$

$$p=11: \quad H_{11} = \left\langle \begin{pmatrix} 0 & 1\\ 10 & 0\end{pmatrix}, \begin{pmatrix} 0 & 4\\ 8 & 10\end{pmatrix}\right\rangle \tag{22}$$

In fact for every prime dimension $p\leq 11$ we can partition $SL(2,\mathbb{Z}_p)$ by using p distinct max-cliques of size p^2-1. For odd primes it suffices to consider the left cosets of H_p in $SL(2,\mathbb{Z}_p)$ where

$$F_t = \begin{pmatrix} 1 & 0\\ t & 1\end{pmatrix} \quad t\in\mathbb{Z}_p \tag{23}$$

are the left coset representatives. For $p=13$ and higher, we were unable to find cliques saturating the upper bound of p^2-1. It is known that, for any primes $p\geq 13$, there does not exist a subgroup H_p of size $|H_p|=p^2-1$ [39], but we are unaware of any proof that cliques of size p^2-1 (i.e. complete BES MUBs for p-dimensional systems) necessarily depend on this subgroup structure. A deterministic search for a clique of size 168 in the $\Gamma(G,T)$ graph for $p=13$ is infeasible, given the computational complexity of the max-clique problem. A heuristic search was able to find a clique of size 158, however.

By adapting a well-known power-of-prime construction for complete MUBs (Bandyopadhyay et al. [11]) we can show that the size of the largest clique satisfies

$$\omega(\Gamma)\geq p(p-1) \quad \forall p \tag{24}$$

To be specific, Section 4.3.1 of [11] describes the construction of a complete set of MUBs for dimensions p^2. In their notation, this amounts to finding a set of p^2 2×2 symmetric matrices $\{A\}$ such that $\det(A_j-A_k)\neq 0$. Suitable sets of matrices are parameterized by two elements $s,t\in\mathbb{Z}_p$ via

$$\{A\} = \left\{ \begin{pmatrix} a & b\\ b & sa+tb\end{pmatrix}, \quad \forall\, a,b\,\in\mathbb{Z}_p\right\} \tag{25}$$

A little thought reveals that every A with non-zero off diagonal element b can be related one-to-one with a matrix $F\in SL(2,\mathbb{Z}_p)$, where F has a non-zero element β (F defined as per Eq. (5)),

$$F(a,b,s,t) = \begin{pmatrix} -ab^{-1} & -b^{-1}\\ b-a^2b^{-1}s-at & -ab^{-1}s-t\end{pmatrix}.$$

One can check that the $\det(A_j-A_k)\neq 0$ condition translates to $\mathrm{Tr}(F_j^{-1}F_k)\neq 2$, as one would expect. In this way we can create a set of $p(p-1)$ matrices $F\in SL(2,\mathbb{Z}_p)$ that form a clique in our Cayley graph $\Gamma(G,T)$. In general, sets of matrices formed this way cannot be extended with an additional

$p-1$ matrices F_k (having $\beta_k = 0$) to form a complete BES MUB i.e., they form (part of) a *maximal*, but not maximum, clique in $\Gamma(G,T)$. However, we can often slightly improve upon the lower bound e.g., we can construct cliques of size $p(p-1)+2$ for primes up 17. A consequence of Eq. (24) is that the fraction of pairs (F_i,F_j) that do not define mutually unbiased bases, out of the total number of such pairs (F_i,F_j), vanishes as $p \to \infty$. In Appendix A, we explicitly give the observables involved in these BES MUBs in terms of tensor products of Pauli operators.

IV. SOME GRAPH-THEORETIC PROPERTIES OF THESE CAYLEY GRAPHS

In this section we further investigate the graph-theoretical properties of the family of Cayley graphs that were previously shown to be closely related to BES MUBs. Without loss of generality, the elements $F \in SL(2,\mathbb{Z}_p)$ can be ordered lexicographically by the vectors constituting the rows of the matrix F i.e.

$$\{F_i\} = \Big\{F_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, F_2 = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \dots$$
$$\dots F_{p(p^2-1)} = \begin{pmatrix} -1 & -1 \\ -1 & -2 \end{pmatrix}\Big\} = \Big\{\begin{pmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{pmatrix}\Big\}.$$

It is easy to see that (i) there are p^2-1 possibilities for $(\alpha,\ \beta)$; (ii) each such $(\alpha,\ \beta)$ in turn allows for p possible $(\gamma,\ \delta)$. Any two elements $F_i,\ F_j$, for which $(\alpha_i,\ \beta_i) = (\alpha_j,\ \beta_j)$, cannot be connected by an edge since

$$\mathrm{Tr}\Big(\begin{pmatrix} \alpha & \beta \\ \gamma_i & \delta_i \end{pmatrix}^{-1}\begin{pmatrix} \alpha & \beta \\ \gamma_j & \delta_j \end{pmatrix}\Big) = \det F_i + \det F_j = 2. \quad (26)$$

The so-called vertex coloring problem for graphs involves assigning a label (color) to every vertex of the graph, such that adjacent vertices cannot be assigned the same color. The minimum number of colors required to do this is the chromatic number, denoted $\chi(\Gamma)$. It is a basic fact [34] that the chromatic number of a graph is bounded below by the clique number i.e. $\omega(\Gamma) \le \chi(\Gamma)$. The discussion leading to Eq. 26 immediately implies that a p^2-1 coloring of the Cayley graph $\Gamma(G,T)$ is possible: assign the same color to two vertices $F_i,\ F_j$ if and only if $(\alpha_i,\ \beta_i) = (\alpha_j,\ \beta_j)$. Since the chromatic number χ is bounded below by the clique number $\omega(\Gamma)$, we know that this coloring is minimal for primes 2 to 11. Hence

$$\omega(\Gamma) = \chi(\Gamma) = p^2-1 \qquad p \in \{2,3,5,7,11\}$$
$$\omega(\Gamma) \le \chi(\Gamma) \le p^2-1 \qquad \forall p$$

Note that the upper bound $\omega(\Gamma) \le p^2-1$ is a graph-theoretical inequality that confirms the geometrical argument preceding Theorem 1 i.e., the number of BES mutually unbiased bases that can fit in a Hilbert space $\mathcal{H}_{p^2} = \mathbb{C}^p \otimes \mathbb{C}^p$ is at most p^2-1.

A concept closely related to cliques and colorings is that of independence. An independent set of a graph is a set of vertices, no two of which are adjacent. A maximum independent set is the largest such set (not necessarily unique) that can be found in the graph, and the independence number, $\alpha(\Gamma)$, of a graph is the size of this maximum independent set. The discussion preceding Eq. (26) can equally well be interpreted as providing a lower bound on the independence number of $\Gamma(G,T)$; there are p^2-1 independent sets of size p, wherein two elements $F_i,\ F_j$ that satisfy $(\alpha_i,\ \beta_i) = (\alpha_j,\ \beta_j)$ are pairwise non-adjacent, hence

$$\alpha(\Gamma) \ge p \qquad \forall p \quad (27)$$

The physical interpretation of this is that we can always find a set of p bases such that, pairwise, no two are mutually unbiased with respect to each other.

The adjacency matrix of a graph Γ with n vertices is an $n \times n$ matrix $A[\Gamma]$ with elements $A_{i,j} = 1$ if vertices i and j are adjacent, and $A_{i,j} = 0$ otherwise. Knowledge of the spectrum of an adjacency matrix often allows us to find, or bound, many quantities of interest. We denote the spectrum of the $p(p^2-1) \times p(p^2-1)$ adjacency matrices $A[\Gamma(G,T)]$ as $\{\lambda_0^{m_0},\lambda_1^{m_1},\lambda_2^{m_2},\lambda_3^{m_3}\}$ where m_i denotes the multiplicity of λ_i. The complement of a graph Γ, denoted $\overline{\Gamma}$, is the graph with same vertex set as Γ, but where two vertices are adjacent in $\overline{\Gamma}$ if and only if they are not adjacent in Γ. The spectrum of a graph and its complement can be related in a simple way for the case of regular graphs (the case we deal with in this work), as the following theorem demonstrates.

Theorem 2 (Brouwer and Haemers [36]) *Suppose Γ is a k-regular graph on n vertices with 4 distinct (adjacency) eigenvalues $\{k = \lambda_0 > \lambda_1 > \lambda_2 > \lambda_3\}$. If, in addition, both Γ and its complement, $\overline{\Gamma}$, are connected, then $\overline{\Gamma}$ also has 4 distinct eigenvalues, $\{n-k-1 > -\lambda_3-1 > -\lambda_2-1 > -\lambda_1-1\}$.*

The Cayley graphs we studied, defined in Eq. (18), are actually the graph complement of a well known family of graphs (that form a family of Ramanujan graphs, amongst other interesting properties), whose spectrum is known exactly.

Theorem 3 (Lubotzky [35]) *Let $G = SL(2,\mathbb{Z}_p)$, and let T (i.e., the connection set for the Cayley graph) be the union of the conjugacy classes c_1 and c_ν of the elements*

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ \nu & 1 \end{pmatrix},$$

where ν is a generator of the cyclic group $\mathbb{Z}_p^* = \mathbb{Z}_p/\{0\}$. Then $T = \{F \in SL(2,\mathbb{Z}_p) | Tr(F) = 2, F \neq I\}$, $|T| = p^2-1$ and the spectrum of the corresponding Cayley graph $A[\Gamma(G,T)]$ denoted $\{\lambda_0^{m_0},\lambda_1^{m_1},\lambda_2^{m_2},\lambda_3^{m_3}\}$, is

$$\begin{aligned} \lambda_0 &= p^2-1, & m_0 &= 1 \\ \lambda_1 &= p-1, & m_1 &= (p-2)(p+1)^2/2 \\ \lambda_2 &= 0, & m_2 &= p^2 \\ \lambda_3 &= -(p+1), & m_3 &= p(p-1)^2/2 \end{aligned}$$

Combining the two preceding theorems (connectedness is obviously satisfied by our Cayley graphs) allows us to completely characterize the spectrum of the canonical Cayley graph Eq. (18) that we used to search for BES MUBs.

Theorem 4 *(Spectrum of graphs defined in Eq. (18)) Let* $G = SL(2,\mathbb{Z}_p)$ *and* $T = \{F \in SL(2,\mathbb{Z}_p) | Tr(F) \neq 2\}$. *Then* $|T| = |G| - p^2$ *and the spectrum of* $A[\Gamma(G,T)]$ *denoted* $\{\lambda_0^{m_0}, \lambda_1^{m_1}, \lambda_2^{m_2}, \lambda_3^{m_3}\}$ *is*

$$\begin{aligned} \lambda_0 &= p(p^2-1)-p^2 & m_0 &= 1 \\ \lambda_1 &= p & m_1 &= p(p-1)^2/2 \\ \lambda_2 &= -1 & m_2 &= p^2 \\ \lambda_3 &= -p & m_3 &= (p-2)(p+1)^2/2 \end{aligned}$$

At this point we note that the problem of finding BES MUBs, framed as finding maximum cliques of size p^2-1 in the Cayley graph Γ defined by Eq. (18), is completely equivalent to finding maximum independent sets of size p^2-1 in the complement, $\overline{\Gamma}$, of that graph i.e.,

$$\exists \text{ complete BES MUB} \iff \omega(\Gamma) = p^2 - 1 = \alpha(\overline{\Gamma}).$$

Unfortunately, it seems that existing spectral lower bounds on the clique number are of little help for the task of proving existence of BES MUBs. Nonetheless, using some well-known spectral bounds we list some implications for the graphs $\Gamma(G,T)$ under consideration. A lower bound on the chromatic number is given by

$$\chi(\Gamma) \geq 1 - \frac{\lambda_0}{\lambda_3} = p(p-1),$$

which, in conjunction with Eq. (26), shows that $p(p-1) \leq \chi(\Gamma) \leq p^2-1$. In fact, this lower bound was already implied by Eq. (24).

For a regular graph, Γ, on n vertices, Hoffman (unpublished) and Lovász [40] proved the formula

$$\alpha(\Gamma) \leq \frac{-n\lambda_{\min}}{\lambda_{\max} - \lambda_{\min}} = \frac{-n\lambda_3}{\lambda_0 - \lambda_3} = p+1,$$

which, in conjunction with Eq. (27) gives us $p \leq \alpha(\Gamma) \leq p+1$. As a final remark on spectral implications, we note that the spectrum exhibited in Thm. 4 classifies $\Gamma(G,T)$ as a so-called walk-regular graph [41].

V. CONCLUSION

We have shown how the set of bipartite entangled stabilizer (BES) states can be partitioned into sets of mutually unbiased bases (MUBs), whose span is sufficient and minimal to describe an interesting class of operators that includes (mixtures of) Jamiołkowski states, Clifford witnesses [7] and more. Mutual unbiasedness of two stabilizer orthonormal bases is easily shown to be equivalent to a simple relation on pairs of matrices from $SL(2,\mathbb{Z}_p)$. Pairs of matrices satisfying this relation are adjacent vertices on a naturally defined Cayley graph, and the problem of finding complete (optimal) BES MUBs is transformed into that of finding maximum cliques in the Cayley graph. In a different mathematical context, the graph complement of our Cayley graphs are well-studied, and so we can quote, for example, the exact spectrum of the adjacency matrix for all prime values p. The most interesting open question is whether such BES-MUBs exist for all primes, or indeed for any primes greater than 11. For the closely related task of finding minimal unitary designs, a discussion by Chau [28] (invoking Dickson's theorem on the existence of certain subgroups of $SL(2,\mathbb{Z}_p)$) suggests that minimal unitary designs only exist for primes up to 11. It remains to be seen whether the latitude afforded by seeking BES-MUBs, as opposed to subgroups of $SL(2,\mathbb{Z}_p)$, allows for construction of optimal BES-MUBs when $p \geq 13$.

Appendix A: Measurement Operators for BES MUBs

Given a matrix $F \in SL(2,\mathbb{Z}_p)$, this defines an orthonormal basis $\mathcal{F}$ in the bipartite Hilbert space $\mathcal{H}_{p^2}$ via

$$\mathcal{F} = \{|J_u^F\rangle, \forall u \in \mathbb{Z}_p^2\}, \quad |\langle J_u^F | J_v^F \rangle| = \delta_{u,v} \qquad \text{(A1)}$$
$$\text{where } |J_u^F\rangle = \left(I \otimes C_{(F|u)}\right) \sum_{j=0}^{p-1} \frac{|jj\rangle}{\sqrt{p}}$$

We will show how the basis $\mathcal{F}$ can be rewritten in terms of stabilizer measurements, and subsequently how $\mathcal{F}$ can be identified as the simultaneous eigenbasis of a set of p^2-1 commuting Pauli operators.

Using so-called symplectic notation, the general form for multi-particle stabilizer operators with vectors $x = (x_1, x_2, \dots)$ and $z = (z_1, z_2, \dots)$ with $x_i, z_i \in \mathbb{Z}_p$ is

$$P_{(x|z)} = (X^{x_1} \otimes X^{x_2} \dots)(Z^{z_1} \otimes Z^{z_2} \dots). \qquad \text{(A2)}$$

Measuring a two-qupit Pauli operator corresponds to projecting with a rank-p projector, Π,

$$\Pi := \Pi_{(x_1,x_2|z_1,z_2)[k]} = \frac{1}{p}\big(I + \omega^{-k} P_{(x_1,x_2|z_1,z_2)} + \dots + \omega^{-(p-1)k} (P_{(x_1,x_2|z_1,z_2)})^{p-1}\big) \qquad \text{(A3)}$$

The product of two appropriately chosen such projectors, Π, Π', defines a rank-1 operator - a stabilizer state:

$$|\psi\rangle\langle\psi| = \frac{1}{p^2} \sum_{s \in \mathcal{G}_s} s = \Pi\, \Pi',$$

where $\mathcal{G}_s = \langle g, g' \rangle$ is a subgroup, generated by two commuting Pauli operators g and g', of the group $\mathcal{G}_2 = \left\{\omega^c P_{(x|z)} | x, z \in \mathbb{Z}_p^2, c \in \mathbb{Z}_p\right\}$. In symplectic notation $g = \omega^{-k} P_{(x_1,x_2|z_1,z_2)}$ and $g' = \omega^{-k'} P_{(x_1',x_2'|z_1',z_2')}$ and commutativity of g and g' reduces to

$$\sum_{i=1,2} x_i z_i - x_i' z_i' \equiv 0 \mod p.$$

Given $u=(u_1,u_2)\in\mathbb{Z}_p^2$ and $\beta\neq 0$, the following two sets of projectors are equal, up to re-ordering

$$\forall u: \quad \left\{|J_u^F\rangle\langle J_u^F|\right\}=\left\{\Pi_{(1,0|\alpha\beta^{-1},-\beta^{-1})[u_1]}\Pi_{(0,1|-\beta^{-1},\beta^{-1}\delta)[u_2]}\right\}.$$

When $\beta=0$, the following two sets of projectors are equal, up to re-ordering

$$\forall u: \quad \left\{|J_u^F\rangle\langle J_u^F|\right\}=\left\{\Pi_{(1,\alpha|0,\gamma)[u_1]}\Pi_{(0,0|1,-\delta)[u_2]}\right\}.$$

Many existing constructions for complete MUBs in $\mathcal{H}_d$ (with power-of-prime dimension d) are based around the partitioning of d^2-1 non-identity Pauli operators into $d+1$ classes, each of which contains $d-1$ mutually commuting operators. Each basis within the MUB is then given by the simultaneous eigenbasis of the $d-1$ mutually commuting operators (i.e., each class is associated with exactly one orthonormal basis, for a given partitioning). We can frame the construction of BES MUBs in this language too, with the modification that we are partitioning the set of all weight-two Pauli operators i.e. the subset $\left\{P_{(x_1,x_2|z_1,z_2)}/\{P_{(x_1,0|z_1,0)},P_{(0,x_2|0,z_2)}\}\right\}$ of size $(p^2-1)^2$. With individual classes containing p^2-1 operators, there can only be at most p^2-1 such classes. It should be clear that a set of n matrices $F\in SL(2,\mathbb{Z}_p)$ (satisfying $\mathrm{Tr}(F_i^{-1}F_j)\neq 2$) is equivalent to n non-overlapping classes of weight-two Pauli operators, each class containing p^2-1 non-identity elements. Recalling Eq. (A1) for the definition of the basis associated with F, then the associated class of unitary operators is the subgroup $\mathcal{G}_s=\langle g,g'\rangle$ of $\mathcal{G}_2$. The simultaneous eigenbasis of all p^2 Pauli operators in $\mathcal{G}_s$ forms an orthonormal basis. When $\beta\neq 0$ the class of Pauli operators corresponding to F is given by

$$\mathcal{G}_s(F)=\langle g,g'\rangle:=\langle P_{(1,0|\alpha\beta^{-1},-\beta^{-1})},P_{(0,1|-\beta^{-1},\beta^{-1}\delta)}\rangle.$$

When $\beta=0$ the class of Pauli operators corresponding to F is given by

$$\mathcal{G}_s(F)=\langle g,g'\rangle:=\langle P_{(1,\alpha|0,\gamma)},P_{(0,0|1,-\delta)}\rangle.$$

[1] R. B. A. Adamson and A. M. Steinberg, "Improving Quantum State Estimation with Mutually Unbiased Bases" Phys. Rev. Lett. **105**, 030406, (2010).

[2] W. K. Wootters and B. D. Fields "Optimal state-determination by mutually unbiased measurements" Ann. Phys. (N.Y.) **191**, 363, (1989).

[3] B. Baumgartner and B. Hiesmayr and H. Narnhofer "A special simplex in the state space for entangled qudits" J. Phys. A. **40**, 7919, (2007).

[4] A. J. Scott, "Optimizing quantum process tomography with unitary 2 -designs" J. Phys. A **41**, number 5, 055308, (2008).

[5] O. Gühne, and P. Hyllus, and D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera "Detection of entanglement with few local measurements", Phys. Rev. A. **66**, 062305, (2002).

[6] Ll. Masanes, "Tight Bell inequality for d-outcome measurements correlations." Quantum Inf. Comput. **3**, pp. 345–358 , (2003).

[7] W. van Dam and M. Howard, "Noise Thresholds for Higher Dimensional Systems using the Discrete Wigner Function" Phys. Rev. A. **83**, 032310, (2011).

[8] E. Bagan, M. Baig, and R. Muñoz-Tapia, "Minimal measurements of the gate fidelity of a qudit map", Phys. Rev. A. **67**, 014303, (2003).

[9] J. Schwinger, "Unitary Operator Bases", Proc. Nat. Acad. Sci., **46**, 570 (1960).

[10] I. D. Ivonovic "Geometrical description of quantal state determination" J. Phys. A. **14**, 3241, (1981).

[11] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, "A New Proof for the Existence of Mutually Unbiased Bases", *Algorithmica*, Volume 34, issue 4, pp. 512–528, (2002).

[12] J. Lawrence, Č. Brukner and A. Zeilinger "Mutually unbiased binary observable sets on N qubits" Phys. Rev. A. **65**, 032320, (2002).

[13] A. B. Klimov, J. L. Romero, G. Björk and L. L. Sánchez-Soto "Geometrical approach to mutually unbiased bases" J. Phys. A. **40**, 3987, (2007).

[14] P. Šulc and J. Tolar "Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions" J. Phys. A. **40**, 15099, (2007).

[15] A. B. Klimov, D. Sych, L. L. Sánchez-Soto and G. Leuchs "Mutually unbiased bases and generalized Bell states" Phys. Rev. A. **79**, 052101, (2009).

[16] A. Kalev, F. C. Khanna and M. Revzen "Partially unbiased entangled bases" Phys. Rev. A. **80**, 022112, (2009).

[17] T. Durt, B.-G. Englert, I. Bengtsson and K. Życzkowski. "On Mutually Unbiased Bases" Int. J. Quantum Information, **8**, 535-640 (2010).

[18] T. Paterek, B. Dakić and C. Brukner "Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models" Phys. Rev. A. **79**, 012109, (2009).

[19] M. Saniga, M. Planat and H. Rosu "Mutually unbiased bases and finite projective planes" J. Opt. B. **6**, L19, (2004).

[20] I. Bengtsson and Å. Ericsson "Mutually Unbiased Bases and the Complementarity Polytope" Open Systems & Information Dynamics **12**, 107, (2005).

[21] W. Wootters "Quantum Measurements and Finite Geometry" Found. Phys. **36**, 112–126, (2006).

[22] E. F. Galvão, "Discrete Wigner functions and quantum computational speedup" Phys. Rev. A. **71**, 042302, (2005).

[23] C. Cormick, E. F. Galvão, D. Gottesman, J. Pablo Paz, and Arthur O. Pittenger , "Classicality in discrete Wigner functions" Phys. Rev. A. **73**, 012301, (2006).

[24] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, "Discrete phase space based on finite fields" Phys. Rev. A. **70**, 062101, (2004).

[25] D. Gross, "Hudson's theorem for finite-dimensional quantum systems" J. Math. Phys. **47**, number 12, 122107, (2006).

[26] W. K. Wootters, "A Wigner-function formulation of finite-state quantum mechanics" Annals of Physics **176**, number 1, pp. 1–21 , (1987).

[27] N. J. Cerf, M. Bourennane, A. Karlsson and N. Gisin, "Security of Quantum Key Distribution Using d-Level Systems"

Phys. Rev. Lett. **88**, 127902, (2002).

[28] H. F. Chau, "Unconditionally secure key distribution in higher dimensions by depolarization" IEEE Trans. Inf. Theory **51**, 1451 , (2005).

[29] D. Gross and K. Audenaert and J. Eisert, "Evenly distributed unitaries: On the structure of unitary designs", J. Math. Phys. **48** number 5, pp. 052104, (2007).

[30] M. Planat, "Pauli graphs when the Hilbert space dimension contains a square: Why the Dedekind psi function?" J. Phys. A **44**, number 4, 045301, (2011).

[31] A. J. Scott and M. Grassl, "Symmetric informationally complete positive-operator-valued measures: A new computer study", J. Math. Phys. **51** number 4, pp. 042203, (2010).

[32] D. M. Appleby, "Properties of the extended Clifford group with applications to SIC-POVMs and MUBs", arXiv:quant-ph/0909.5233, (2009).

[33] D. M. Appleby, I. Bengtsson and S. Chaturvedi, "Spectra of phase point operators in odd prime dimensions and the extended Clifford group", J. Math. Phys. **49** number 1, pp. 012102, (2008).

[34] P. J. Cameron, J. H. van Lint, "Graph Theory, Coding Theory and Block Designs", Cambridge Univ. Press, Cambridge, (1975).

[35] A. Lubotzky. "Discrete Groups, Expanding Graphs and Invariant Measures", Birkhäuser, 1994. ISBN 3 7643 5075 X.

[36] A. E. Brouwer, W. H. Haemers, Spectra of graphs, Unpublished course notes. Available from: `http://homepages.cwi.nl/~aeb/math/ipm.pdf`.

[37] A. Hibbard and K. Levasseur, "Exploring Abstract Algebra with Mathematica (EAAM)', Exploring Abstract Algebra with Mathematica (EAAM) Springer-Verlag, New York (as part of the TELOS imprint), (1998). `http://www.central.edu/EAAM/`

[38] The GAP Group, *GAP – Groups, Algorithms, and Programming,Version 4.4.12*, (2008). `http://www.gap-system.org`.

[39] L. E. Dickson, Linear Groups: With An Exposition Of The Galois Field Theory. New York: reprinted edition by Dover, 1958. 260.

[40] L. Lovász "On the Shannon capacity of a graph", IEEE Transactions on Information Theory **25** number 1, pp. 1–7, (1979).

[41] C. D. Godsil and B. D. McKay "Feasibility conditions for the existence of walk-regular graphs", Linear Algebra and its Applications **30** pp. 51–61, (1980).